**IN THE UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF OREGON**

| | |
|---|---|
| IN RE: PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION | Case No. 3:15-md-2633-SI |
| This Document Relates to All Actions. | **OPINION AND ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS** |

Kim D. Stephens, Christopher I. Brain, Chase C. Alvord, and Jason T. Dennett, TOUSLEY BRAIN STEPHENS PLLC, 1700 Seventh Avenue, Suite 2200, Seattle, WA 98101; Keith S. Dubanevich, Steve D. Larson, and Mark A. Friel, STOLL STOLL BERNE LOKTING & SHLACHTER PC, 209 SW Oak Street, Portland, OR 97204; Ari J. Scharg, EDELSON PC, 350 North LaSalle Street, Suite 1300, Chicago, IL 60654; Tina Wolfson, AHDOOT AND WOLFSON PC, 1016 Palm Avenue, West Hollywood, CA 90069; and James Pizzirusso, HAUSFELD LLP, 1700 K Street NW, Suite 650, Washington, DC 20006. Of Attorneys for Plaintiffs.

Daniel R. Warren, BAKERHOSTETLER LLP, 1900 East Ninth Street, Suite 3200, Cleveland, OH 44114; Paul G. Karlsgodt, BAKERHOSTETLER LLP, 1801 California Street, Suite 4400, Denver, CO 80202; and Darin M. Sands, LANE POWELL PC, 601 SW Second Avenue, Suite 2100, Portland, OR 97204. Of Attorneys for Defendant Premera Blue Cross.

**Michael H. Simon, District Judge.**

Plaintiffs bring this putative class action against Defendant Premera Blue Cross ("Premera"), a healthcare benefits provider. On March 17, 2015, Premera publicly disclosed that its computer network had been breached. Plaintiffs allege that this breach compromised the

confidential information of approximately 11 million current and former members, affiliated members, and employees of Premera. The compromised confidential information includes names, dates of birth, Social Security Numbers, member identification numbers, mailing addresses, telephone numbers, email addresses, medical claims information, financial information, and other protected health information (collectively, "Sensitive Information"). According to Plaintiffs, the breach began in May 2014, and went undetected for almost a year. Plaintiffs further allege that after discovering the breach, Premera waited several months before notifying all affected individuals. Based on these allegations, among others, Plaintiffs assert that they have been damaged in several ways and bring various common law claims and state statutory claims. Premera moves to dismiss several of Plaintiffs' claims and several of Plaintiffs' damage theories. For the reasons that follow, the Court grants Premera's motion in part, denies Premera's motion in part, and gives Plaintiffs leave to replead.

**STANDARDS**

A motion to dismiss for failure to state a claim may be granted only when there is no cognizable legal theory to support the claim or when the complaint lacks sufficient factual allegations to state a facially plausible claim for relief. *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010). In evaluating the sufficiency of a complaint's factual allegations, the court must accept as true all well-pleaded material facts alleged in the complaint and construe them in the light most favorable to the non-moving party. *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1140 (9th Cir. 2012); *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010). To be entitled to a presumption of truth, allegations in a complaint "may not simply recite the elements of a cause of action, but must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011). All reasonable inferences from

the factual allegations must be drawn in favor of the plaintiff. *Newcal Indus. v. Ikon Office Solution*, 513 F.3d 1038, 1043 n.2 (9th Cir. 2008). The court need not, however, credit the plaintiff's legal conclusions that are couched as factual allegations. *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009).

A complaint must contain sufficient factual allegations to "plausibly suggest an entitlement to relief, such that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." *Starr*, 652 F.3d at 1216. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007)).

## BACKGROUND

Plaintiffs allege the following facts, among others, in their Consolidated Class Action Allegation Complaint ("Compl.") (ECF 44):

### A. The Parties

Premera is one of the largest healthcare benefits companies in the Pacific Northwest and is also a participant in the national Blue Cross Blue Shield Association (which offers healthcare benefits to consumers throughout the United States and its territories, covering more than 105 million Americans). Premera's participation in the Blue Cross Blue Shield Association provides its members with access to healthcare providers throughout the country and provides non-Premera Blue Cross members (referred to as "Blue members") with access to its network. Compl. ¶ 2. To become a Premera member (or, for Blue members, receive healthcare services from a provider within the Premera network), an individual must give Premera his or her Sensitive Information. Plaintiffs and the putative class took reasonable steps to preserve the confidentiality of their Sensitive Information in many ways, including protecting the Sensitive

Information with confidential passwords and relying upon physician-patient privilege and confidentiality. Premera maintains this Sensitive Information in a centralized database. Compl. ¶ 3. As a healthcare insurance provider, Premera is required to protect both its members' and also Blue members' Sensitive Information, including by adopting and implementing specific data security regulations and standards set forth under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Compl. ¶ 4.

Plaintiffs allege a Nationwide Data Breach Class, consisting of "[a]ll persons in the United States whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015." Compl. ¶ 101. Plaintiffs also allege a Nationwide Premera Policyholder Subclass, consisting of "[a]ll Nationwide Data Breach Class members who paid money to Premera prior to March 17, 2015 in exchange for health insurance" ("Policyholder Plaintiffs") Compl. ¶ 102.[1] The individually-named Plaintiffs are identified and alleged to be members of one or more classes or subclasses. Compl. ¶¶ 12-34, 101-102, 105-109.

**B. The Data Breach**

On March 17, 2015, Premera revealed that its computer network had been breached and the Sensitive Information of approximately 11 million of its former and current members, Blue members, and employees was compromised. Compl. ¶ 6. According to Premera, the breach started in May 2014 and went undetected for nearly one year. In addition, after discovering the breach, Premera waited several months before notifying all affected individuals. Compl. ¶¶ 7, 59.

[1] Plaintiffs also allege certain state-specific classes and subclasses. Compl. ¶¶ 104-108. These distinctions are not relevant to the pending motion. In addition, Plaintiffs excluded certain people and entities from the proposed classes and subclasses. Compl. ¶ 110. These exclusions are not relevant to the pending motion.

On April 8, 2014, approximately one month *before* the Premera breach, the Cyber Division of the Federal Bureau of Investigation ("FBI") issued a Private Industry Notification to companies within the healthcare sector, advising that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." Compl. ¶ 43 (footnoted citation omitted).

In addition, several weeks *before* the Premera breach, the U.S. Office of Personnel Management directly notified Premera about its specific network security vulnerabilities. The U.S. Office of Personnel Management's report dated April 18, 2014 revealed that Premera failed to implement adequate measures to secure its network. It found "several areas of concern related to Premera's network security controls" and noted that "patches are not being implemented in a timely manner," "a methodology is not in place to ensure that unsupported or out-of-date software is not utilized," and a vulnerability scan identified "insecure server configurations." Compl. ¶ 44 (citations omitted). In sum, the federal auditors notified Premera weeks before the breach that its network-security procedures were inadequate and informed Premera that some of the vulnerabilities could be exploited by hackers and expose sensitive information. Compl. ¶ 45 (citation omitted).

On May 5, 2014, hackers began the initial attack on Premera's servers. A "phishing" email was sent to a Premera employee, falsely purporting to be from a Premera Information Technology (IT) employee. The email included instructions to download a "security update." Premera's employee downloaded this "update," which actually was malware that allowed

hackers access to Premera's servers. Compl. ¶ 46. The hackers used the domain name in their email of "premrera.com" (*i.e.*, using an additional "r"). This wrong domain name was visible in the email message. Around this same time, another phishing domain of "prennera.com" also was registered. Compl. ¶ 48. After the Premera employee downloaded the malware, hackers had access to at least two of Premera's servers for many months. This access went undetected by Premera. Compl. ¶ 49.

In October 2014, Premera engaged Mandiant, a cyber-security firm, to perform an assessment of the security of Premera's network. Mandiant provided its agents with Mandiant Intelligent Response ("MIR"), a tool used to identify indicators of compromise and malware, to install on Premera's workstations and laptops for the purposes of scanning for malware and other infections. The pilot phase of this project began in December 2014 and continued until early January 2015. During this time, Premera began installing MIR on workstations and laptops. Premera did not install network sensors until January 28, 2015. On January 29, 2015, Mandiant discovered a signature for "SOGU" malware traffic on the Premera network, confirmed infection of two servers, and confirmed that the malware was "beaconing" to attacker sites. By January 30, 2015, Premera had uncovered that the SOGU malware had been in its system since May 2014. Compl. ¶¶ 50-52.

In February 2015, Mandiant continued to try to learn the full extent of the breach and whether—or how much—information had been removed from Premera's system. At this time, Premera deployed Mandiant's tools on all Premera servers, workstations, and laptops in order to assess the scope of the breach. This installation was completed in late February, nearly one month after Premera first discovered that a breach had occurred. On February 20, 2015, Premera notified the FBI of the data breach.

On February 25, 2015, the FBI met with Premera and Mandiant. The FBI then began its own investigation. Premera chose not to inform the public of the breach at this time, deciding instead to investigate further and attempt to remediate the breach before letting the public know that their Sensitive Information had been stolen (and was continuing to be stolen). Premera further waited until the weekend of March 6-8, 2015 to perform the complete remediation of its network, during which time information was still being accessed and stolen. Mandiant continued to monitor the network for the following week to ensure that Premera had completely cleansed its system. Compl. ¶¶ 53-56.

On March 17, 2015, Premera disclosed to the public that a massive data breach had occurred. In its notice, Premera revealed that its computer network was the target of "a sophisticated attack to gain unauthorized access to [Premera's] Information Technology (IT) systems." As a result, the Sensitive Information belonging to approximately 11 million consumers—including its current and former members, employees, and other Blue members—was compromised. The breach affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and affiliate brands Vivacity and Connexion Insurance Solutions, Inc. The breach also affected members of other Blue Cross Blue Shield plans who sought treatment in Washington, Oregon, or Alaska. Compl. ¶¶ 57-58 (citation omitted; typographical error regarding year corrected).

**C. Plaintiffs' Causes of Action**

Plaintiffs allege that Premera's data security failures demonstrate that, among other things, Premera failed to: maintain an adequate data security system; adequately protect Plaintiffs' and the Classes' Sensitive Information; ensure the confidentiality of the Sensitive Information that Premera created, received, maintained, and transmitted; implement appropriate technical policies and procedures; and effectively train all members of its workforce.

Compl. ¶ 64. Based on these allegations, Plaintiffs assert the following eleven causes of action: (1) violation of the Washington Consumer Protection Act ("CPA"), RCW §§ 19.86.010, *et seq.*;[2] (2) violation of the Washington Data Breach Disclosure Law, RCW § 19.255.010;[3] (3) negligence;[4] (4) breach of express contract;[5] (5) breach of implied contract;[6] (6) restitution or unjust enrichment;[7] (7) violation of various state consumer protection laws;[8] (8) violation of various state data breach notification laws;[9] (9) violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code §§ 56, *et seq.*;[10] (10) breach of fiduciary duty;[11] and (11) misrepresentation by omission (through fraudulent, negligent, or reckless omission or concealment).[12]

**D. Plaintiffs' Alleged Damages**

Plaintiffs allege three categories of injury or damage. First, Plaintiffs allege "out of pocket" losses related to credit monitoring expenses, fraudulent accounts or tax returns, loss of use of money, and time and effort that Plaintiffs spent responding to the compromise of their

[2] Compl. ¶¶ 119-139.

[3] Compl. ¶¶ 140-144.

[4] Compl. ¶¶ 145-159.

[5] Compl. ¶¶ 160-174.

[6] Compl. ¶¶ 175-185.

[7] Compl. ¶¶ 186-191.

[8] Compl. ¶¶ 192-205.

[9] Compl. ¶¶ 206-212.

[10] Compl. ¶¶ 213-217.

[11] Compl. ¶¶ 218-228.

[12] Compl. ¶¶ 229-237.

Sensitive Information. Some of these losses are monetary and others are only for the time and effort that had to be expended. Second, Plaintiffs allege damages inherent in the value of their personal information and the violation of their right to privacy. Third, the Policyholder Plaintiffs, who paid money to Premera as premiums for insurance coverage, including what the Policyholder Plaintiffs assert was for data security, allege "benefit of the bargain" damages. Related to this third category of damage, Plaintiffs allege that had Premera disclosed its "true" data security practices, the Policyholder Plaintiffs never would have purchased their health insurance from Premera in the first place. *See, e.g.*, Compl. ¶¶ 78-100, 127-137.[13] *See also* Plaintiffs' Response in Opposition to Premera's Motion to Dismiss ("Response") (ECF 53) at 13.[14]

**DISCUSSION**

Invoking Rule 12(b)(6) of the Federal Rules of Civil Procedure in its Motion to Dismiss ("Motion") (ECF 49), Premera challenges only certain causes of action and only certain damage theories alleged by Plaintiffs. Plaintiffs' unchallenged claims and damage theories are not addressed by the Court at this time.[15]

[13] For purposes of resolving the pending motion, the Court does not consider it necessary to focus on which specifically-named Plaintiffs allege which claims or allegedly suffered which damages.

[14] Page numbers are cited to the ECF pagination and not to the internal pagination within the filed document.

[15] Many district courts have held that a motion to dismiss filed by a defendant that is directed against less than all of the claims alleged by a plaintiff suspends the time for that defendant to answer the unchallenged claims. *See, e.g.*, *ThermoLife Int'l, LLC v. Gaspari Nutrition, Inc.*, 2011 WL 6296833, at *5 (D. Ariz. Dec. 16, 2011). This Court follows that approach.

**A. Plaintiffs' Fraud-Based Claims**

In its Motion, Premera challenges the allegations of fraud contained in Plaintiffs' First Claim (Washington CPA), Seventh Claim (other state consumer protection laws), and Eleventh Claim (Misrepresentation by Omission). Premera argues that Plaintiffs' allegations of fraud fail to comply with the heightened pleading requirements of Rule 9(b) of the Federal Rules of Civil Procedure. Plaintiffs respond that their claims do not "sound in fraud" and thus are not subject to Rule 9(b). Plaintiffs further respond that even if Rule 9(b) did apply to Plaintiffs' allegations of fraud, Plaintiffs' Complaint is sufficient to satisfy Rule 9(b).

**1. All Allegations of Fraud Are Subject to Rule 9(b)**

Rule 9(b) provides:

> In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Malice, intent, knowledge, and other conditions of a person's mind may be alleged generally.

Fed. R. Civ. P. 9(b). This rule applies not only to federal causes of action, but also to state-law causes of action alleged in federal court. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103 (9th Cir. 2003); *see also Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). "The Federal Rules of Civil Procedure apply irrespective of the source of subject matter jurisdiction, and irrespective of whether the substantive law at issue is state or federal." *Vess*, 317 F.3d at 1102, citing *Hanna v. Plumer*, 380 U.S. 460 (1965).

In addition, Rule 9(b) applies to all allegations, or averments, of fraud in all civil cases in federal court, even when fraud is not an essential element of the claim. As explained by the Ninth Circuit in *Vess*:

> In cases where fraud is not a necessary element of a claim, a plaintiff may choose nonetheless to allege in the complaint that the defendant has engaged in fraudulent conduct. In some cases, the plaintiff may allege a unified course of fraudulent conduct and rely

> entirely on that course of conduct as the basis of a claim. In that event, the claim is said to be "grounded in fraud" or to "sound in fraud," and the pleading of that claim as a whole must satisfy the particularity requirement of Rule 9(b). . . .
>
> In other cases, however, a plaintiff may choose not to allege a unified course of fraudulent conduct in support of a claim, but rather to allege some fraudulent and some non-fraudulent conduct. In such cases, only the allegations of fraud are subject to Rule 9(b)'s heightened pleading requirements. The text of Rule 9(b) requires only that in "all *averments of fraud* . . ., the circumstances constituting fraud . . . shall be stated with particularity." Fed.R.Civ.P. 9(b) (emphasis added).[16] The rule does not require that allegations supporting a claim be stated with particularity when those allegations describe non-fraudulent conduct.
>
> In such cases, application of Rule 9(b)'s heightened pleading requirements only to "averments" of fraud supporting a claim rather than to the claim as a whole not only comports with the text of the rule; it also comports with the rule's purpose of protecting a defendant from reputational harm. . . . Fraud allegations may damage a defendant's reputation regardless of the cause of action in which they appear, and they are therefore properly subject to Rule 9(b) in every case. To require that non-fraud allegations be stated with particularity merely because they appear in a complaint alongside fraud averments, however, serves no similar reputation-preserving function, and would impose a burden on plaintiffs not contemplated by the notice pleading requirements of Rule 8(a).
>
> * * *
>
> Thus, if particular averments of fraud are insufficiently pled under Rule 9(b), a district court should "disregard" those averments, or "strip" them from the claim. The court should then examine the allegations that remain to determine whether they state a claim.

*Vess*, 317 F.3d at 1103-05 (emphasis in original).

---

[16] An "averment" is a positive declaration or affirmation of fact; an assertion or allegation in a pleading is an averment. Bryan A. Garner, ed., BLACK'S LAW DICTIONARY 156 (9th ed. 2009). In 2007, the text of Rule 9 was amended to make it "more easily understood. . . . These changes are intended to be stylistic only." Fed. R. Civ. P. 9 advisory committee's note 59 2007 amendment. Thus, the change from "averments of fraud" to "alleging fraud" does not affect this analysis.

**2. Whether Plaintiffs' Complaint Satisfies Rule 9(b)**

Premera identifies four paragraphs in which it asserts that Plaintiffs allege fraud. In their First Claim (Washington CPA), Plaintiffs allege, among other things, that Premera "actively concealed its true security practices from Plaintiffs." Compl. ¶ 126. Similarly, in their Seventh Claim (other state consumer protection laws), Plaintiffs allege, among other things, that Premera "actively concealed its true security practices from Plaintiffs." Compl. ¶ 197. Further, in their Eleventh Claim (Misrepresentation by Omission), Plaintiffs allege that Premera acted "fraudulently, negligently, or recklessly concealed from, or failed to disclose to," the alleged Class "the fact that the measures it employed to protect consumers' confidential data from hackers were insufficient." Compl. ¶ 231. Finally, also in their Eleventh Claim, Plaintiffs allege that Premera "intentionally, recklessly, or negligently concealed or failed to disclose the insufficient nature of its security measures for the purpose of inducing" the Class to act thereon and that the Class members "justifiably relied to their detriment upon the truth and completeness of Premera's representations." Compl. ¶ 234.

**a. Fraud through affirmative misrepresentation**

It is unclear in the Complaint whether Plaintiffs intended to allege that Premera committed fraud through affirmative misrepresentations. In their First Claim (and by extension their Seventh Claim), Plaintiffs allege that Premera made certain promises in its Notice of Privacy Practices, Code of Conduct, public statements, and other (unspecified) "written understandings" to safeguard and protect Sensitive Information. Compl. ¶ 123. Plaintiffs further allege that Premera "knew (or should have known) that it was not adequately protecting Plaintiffs' . . . Sensitive Information." Compl. ¶ 126. Together, these allegations may be construed to allege fraud by making promises that a party knew it did not intend to keep. *See also* Compl. ¶¶ 40-42. In Plaintiffs' Response, Plaintiffs argue that they have identified

actionable misrepresentations with sufficient particularity, and they refer back to the allegations in ¶¶ 40-42. Response at 25-26.

Neither a court nor a defendant should be required to guess whether a plaintiff is alleging fraud through affirmative misrepresentation. Therefore, to the extent that Plaintiffs seek to allege fraud through affirmative misrepresentation, any such claims in the current Complaint are dismissed with leave to replead. If Plaintiffs want to allege that Premera committed fraud through affirmative misrepresentation, Plaintiffs must clearly and explicitly allege each specific misrepresentation that Plaintiffs contend Premera fraudulently made, along with all of the other matters required under Rule 9(b) for pleading an allegation of fraud through affirmative misrepresentation.

**b. Active concealment**

Plaintiffs allege in their First, Seventh, and Eleventh Claims theories of active concealment, among other theories. Active concealment is a species of fraud. It requires more than merely failing to own up to the truth. *Grimmett v. Brown*, 75 F.3d 506, 515 (9th Cir. 1996). It also requires more than merely making an affirmative misrepresentation, because, if it were otherwise, then there would be no point in having a separate doctrine of active concealment. Were a plaintiff to allege that a defendant contacted the plaintiff and intentionally misled or gave materially incorrect information to the plaintiff in order to send that party down the wrong path, this would suffice as an allegation of active concealment. *See In re Toyota Motor Corp. Unintended Acceleration Marketing, Sales Practices, and Prods. Liab. Litig.*, 754 F. Supp. 2d 1145, 1192 (C.D. Cal. 2010).

In their Complaint, however, Plaintiffs merely assert "active concealment" in a conclusory fashion. Although Plaintiffs allege that Premera "actively concealed its true security practices from Plaintiffs," Compl. ¶¶ 126, 197, Plaintiffs do not allege how Premera engaged in

such "active concealment." Plaintiffs allegations are insufficient. Therefore, any claims of active concealment in the Complaint are dismissed with leave to replead. If Plaintiffs want to allege that Premera committed fraud through active concealment, Plaintiffs must clearly and explicitly allege what Premera did that constitutes active concealment, beyond merely making an affirmative misrepresentation or omitting to disclose material information.

**c. Fraud by omission**

To the extent that Plaintiffs' Eleventh Claim alleges negligent omission or failure to disclose, such allegations are not subject to the heightened pleading standards of Rule 9(b) and are not the subject of Premera's pending motion. To the extent that Plaintiffs' Eleventh Claim alleges active concealment (whether done fraudulently, negligently, or recklessly), it is subject to the same ruling stated above for fraudulent active concealment. Finally, to the extent that Plaintiffs' Eleventh Claim alleges fraud by material omission, it is subject to Rule 9(b), although in a less strict form. As Judge Lucy Koh recently explained in another data breach lawsuit involving another provider of healthcare benefits:

> In most cases, "a plaintiff in a fraud by omission suit will not be able to specify the time, place, and specific content of an omission as precisely as would a plaintiff in a false representation claim." *Falk v. Gen. Motors Corp.*, 496 F. Supp. 2d 1088, 1098–99 (N.D. Cal. 2007); *see also Gold v. Lumber Liquidators, Inc.*, 2015 WL 7888906, *10 (N.D. Cal. Nov. 30, 2015) (same). Accordingly, "a fraud by omission or fraud by concealment claim can succeed without the same level of specificity required by a normal fraud claim." *Baggett v. Hewlett-Packard Co.*, 582 F. Supp. 2d 1261, 1267 (C.D. Cal. 2007) (internal quotation marks omitted); *accord MacDonald v. Ford Motor Co.*, 37 F. Supp. 3d 1087, 1096 (N.D. Cal. 2014) ("[C]laims based on an omission can succeed without the same level of specificity required by a normal fraud claim[,]. . . [b]ecause the plaintiffs are alleging a failure to act instead of an affirmative act.") (internal quotation marks and alteration omitted); *Montich v. Miele USA, Inc.*, 849 F. Supp. 2d 439, 451 (D.N.J. 2012) ("[The] heightened [pleading] standard [under Rule 9(b)] is somewhat relaxed in a case based on a fraudulent omission.").

*In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *35 (N.D. Cal. May 27, 2016) (brackets in original).

In the present case, Plaintiffs allege that had Premera disclosed its "true" data security practices, the Policyholder Plaintiffs never would have purchased their health insurance from Premera in the first place. *See, e.g.*, Compl. ¶¶ 78-100, 127-137. This is a sufficient allegation of materiality and reliance. In addition, the duty to speak and to avoid making a material omission also is sufficiently alleged. Plaintiffs allege that Premera made certain promises in its Notice of Privacy Practices, Code of Conduct, and other public statements that it would safeguard and protect Sensitive Information. Compl. ¶ 123. At least at the pleading stage, these statements are sufficient to give rise to a duty to speak to avoid fraudulently making a half-truth.[17]

What is missing, however, from Plaintiffs' allegations is a clear articulation of precisely what should have been disclosed to Plaintiffs in order to prevent making the statements that Premera did make from being misleading, *i.e.* a half-truth. Accordingly, any claims of fraud by omission (or by half-truth) in the Complaint are dismissed with leave to replead. If Plaintiffs want to allege that Premera committed fraud through omission, Plaintiffs must clearly and explicitly allege what Premera omitted, namely what Premera should have disclosed in order to avoid making a half-truth or otherwise being misleading.

**B. Plaintiffs' Contract-Based Claims**

In its Motion, Premera challenges Plaintiffs' Fourth Claim (Breach of Express Contract), Fifth Claim (Breach of Implied Contract), and Sixth Claim (Restitution/Unjust Enrichment). Premera refers to these three claims as Plaintiffs' "contract-based" claims.

[17] *See generally Benson Tower Condo. Ass'n v. Victaulic Co.*, 2014 WL 5285475, at *12-14 (D. Or. Oct. 15, 2014) (discussing Oregon's law of fraud by half-truths).

**1. Plaintiffs' Fourth Claim (Breach of Express Contract)**

Premera argues that the Policyholder Plaintiffs fail to allege sufficient facts plausibly to establish that their contracts with Premera contain any promise at all regarding data security. Plaintiffs allege that the Policyholder Plaintiffs "entered into valid and enforceable contracts with Defendant whereby it promised to provide healthcare and data protection services to them" and that the Policyholder Plaintiffs "agreed to, among other things, pay money for such services." Compl. ¶ 161. Plaintiffs also allege that both the provision of healthcare and data protection services were "material." Compl. ¶ 162. Premera then argues that Plaintiffs did not cite, attach, quote from, or even reference their particular health insurance "contracts" (or any exemplar contract) to support their claim of breach of express contract.

Instead, Plaintiffs refer to Premera's "Notice of Privacy Practices, Code of Conduct, public statements, and other written understandings," in which, Plaintiffs allege, Premera "expressly promised . . . to safeguard and protect the confidentiality of [Plaintiffs'] Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards." Compl. ¶ 163. Plaintiffs further allege that Premera "did not comply with its promises to abide by HIPAA, federal, state and local laws, or industry standards," and that the "failure to meet these promises and obligations constitutes a breach of express contract." Compl. ¶¶ 166-167.

Although Plaintiffs did not attach to its Complaint copies of Premera's Notice of Privacy Practices and Code of Conduct, they did quote portions of these documents and provide web addresses showing where these documents could be found. Compl. ¶¶ 40-41. Premera attached to its Motion a copy of its Notice of Privacy Practices dated November 20, 2015 (ECF 49-1) and its

Code of Conduct dated May 2015 (ECF 49-2). These documents may be considered by the Court in ruling on Premera's Motion.[18]

Premera argues that a threshold question is whether either Prermera's Notice of Privacy Practices or its Code of Conduct is part of the health benefits "contract" between the Policyholder Plaintiffs and Premera. Premera argues that Plaintiffs do not explain how documents that Plaintiffs "never saw or understood as an offer could form the basis of an express contractual relationship between the parties." Motion at 19. In response, Plaintiffs assert that they have alleged the requisite contractual elements of offer, acceptance, and consideration, including that Premera promised to provide healthcare and data protection services and reduced those promises to writing in several documents, including its Notice of Privacy Practices and Code of Conduct. Plaintiffs argue that "[n]othing more is required at the pleading stage," citing *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1329 (11th Cir. 2012). Response at 29. In reply, Premera notes that in *Resnick*, the plaintiffs had attached a written "service contract" to their complaint, which the court relied upon in finding that an express contract existed between the parties. Premera's Reply Brief ("Reply") (ECF 54) at 16.

In *Resnick*, current or former members of health care plans brought an action against the plan operator, relating to identity theft incidents that occurred after unencrypted laptops

[18] As a general rule, a district court may not consider any material beyond the pleadings in ruling on a motion under Rule 12(b)(6) of the Federal Rules of Civil Procedure. *Lee v. City of Los Angeles*, 250 F.3d 668, 688-89 (9th Cir. 2001). When matters outside the pleadings are presented to the court, a motion to dismiss generally must be converted to a motion for summary judgment under Rule 56, with the parties being given an opportunity to present all pertinent material. Fed. R. Civ. P. 12(d). There are, however, two exceptions to this rule. First, a court may consider "material which is properly submitted as part of the complaint." *Lee*, 250 F.3d at 688. This includes both documents physically attached to the complaint and those on which the complaint "necessarily relies" whose authenticity is not contested. *Id*. Second, the court may take judicial notice of "matters of public record" pursuant to Rule 201(b) of the Federal Rules of Evidence without being required to convert the Rule 12(b)(6) motion into a motion for summary judgment under Rule 56. *Lee*, 250 F.3d at 688–89.

containing members' sensitive information were stolen from the plan operator's corporate office. The plaintiffs asserted claims under Florida law for negligence, negligence *per se*, breach of contract, breach of implied contract, breach of implied covenant of good faith and fair dealing, breach of fiduciary duty, and restitution or unjust enrichment. The district court granted the defendant's motion to dismiss for failure to state a claim, and the Eleventh Circuit reversed in part and affirmed in part. Regarding the plaintiffs' claim of breach of express contract, the Eleventh Circuit held that the complaint was sufficient. In affirming the district court's dismissal of the plaintiffs' claim of breach of the implied covenant of good faith and fair dealing, the Eleventh Court stated:

> Plaintiffs here allege that AvMed breached the *express provision of the service contract*, which required AvMed "to ensure the 'confidentiality of information about members' medical health condition being maintained by the Plan and the right to approve or refuse the release of member specific information including medical records, by AvMed, except when the release is required by law.'"

*Resnick*, 693 F.3d at 1329 (emphasis added). Unlike in *Resnick*, Plaintiffs here do not allege that Premera violated any *express* provision of its health benefits contract with the Policyholder Plaintiffs. Instead, Plaintiffs allege that "they entered into valid and enforceable contracts with Defendant whereby it promised to provide healthcare and data protection services to them." Compl. ¶ 161. Premera argues that Plaintiffs do not identify any express provision in the parties' health benefits contracts that contains any promise relating to data security and that Plaintiffs' references to Premera's Notice of Privacy Practices and Code of Conduct only gives rise to the question of whether those documents are part of the parties' health benefits contract. Premera's argument is well-taken.

Premera's point can be seen most clearly in the recent decision by Judge Koh in the *Anthem* data breach litigation, which also involved claims by policyholders against their health

benefits provider and others, related to a data breach and compromise of sensitive personal information. Regarding the claim for breach of contract under California law asserted by the plaintiffs in their Second Consolidated Amended Complaint ("SAC") in *Anthem*, Judge Koh observed:

> For California Plaintiffs covered by an individual or fully-insured group plan, the Anthem Defendants contend that, although "[t]he SAC asserts that various privacy notices and policies became enforceable provisions of Plaintiffs' health plan contracts," the SAC "fails to allege facts to support th[is] assertion." Anthem Mot. at 6. California Plaintiffs, in response, assert that these privacy provisions were part of their underlying contracts via incorporation by reference or through express attachment.
>
> a. **Incorporation by Reference**
>
> As to incorporation by reference, California law provides that "[a] contract may validly include the provisions of a document not physically a part of the basic contract." *Shaw v. Regents of Univ. of Cal*., 67 Cal. Rptr. 2d 850, 856 (Ct. App. 1997). "It is, of course, the law that the parties may incorporate by reference into their contract the terms of some other document." *Id*. "For the terms of another document to be incorporated into the document executed by the parties (1) the reference must be clear and unequivocal, (2) the reference must be called to the attention of the other party and he must consent thereto, and (3) the terms of the incorporated document must be known or easily available to the contracting parties." *Id*. "The contract need not recite that it incorporates another document, so long as it guides the reader to the incorporated document." *Id*. (internal quotation marks and alteration omitted).
>
> * * *
>
> Under *Shaw* and *Wolschlager*, the contracts entered into by Michael Bronzo ("Bronzo"), Kenneth Solomon ("Solomon"), Mary Ella Carter ("Carter"), and Kenneth Coonce ("Coonce") sufficiently incorporate by reference the Anthem Defendants' promises to protect individual privacy.

*Anthem*, 2016 WL 3029783, at *8-9. The court in *Anthem* then found that the plaintiffs adequately alleged that the references in their health benefits contract to Anthem's privacy

notices and policies were clear and unequivocal, those references were called to the attention of the plaintiffs, and the terms of the incorporated documents were known or easily available to the contracting parties. *Id.* at *9-10.

In their lawsuit against Premera, the Policyholder Plaintiffs do not explicitly allege that Premera's privacy notices or policies (from which Plaintiffs quote in paragraphs 40 and 41 of the Complaint) were part of the Policyholder Plaintiffs' health benefits contracts with Premera, either through "incorporation by reference" or through "express attachment." In that respect, Plaintiffs' allegations are deficient and their breach of express contract claim is dismissed with leave to renew. If Plaintiffs intend to allege that Premera's privacy notices, policies, commitments, or provisions were incorporated by reference into Plaintiffs' health benefits contracts, Plaintiffs must allege the specific provisions within those contracts showing that: (1) the reference was clear and unequivocal; (2) the reference was called to the attention of the other party, and (3) the terms of the incorporated documents were easily available to the contracting parties.

As discussed more fully in the next subsection, it is unclear whether the Policyholder Plaintiffs also intended to allege breach of express contract where the referenced confidentiality provisions are an *implied* term in the parties' express contracts. If that is Plaintiffs' intention, they have leave to replead such a claim, including as an alternative theory of breach of express contract.

**2. Plaintiffs' Fifth Claim (Breach of Implied Contract)**

As an alternative to their claim of breach of express contract, the Policyholder Plaintiffs allege breach of implied contract. Specifically, these Plaintiffs allege that they provided Sensitive Information to Premera and thereby "entered into implied contracts whereby Defendant was obligated to take reasonable steps to secure and safeguard that information." Compl. ¶ 177.

Plaintiffs add that without having such implied contracts, Plaintiffs "would not have provided their Sensitive Information to Defendant." Compl. ¶ 179. Premera challenges Plaintiffs' claim of breach of implied contract by arguing that even for an implied contract claim, the basic elements of offer, acceptance, and mutual assent still must be met. Motion at 21. Plaintiffs respond that the "specific facts and circumstances of the transaction between Premera and the Policyholder Plaintiffs culminated in a meeting of the minds, wherein the parties understood there to be an offer, acceptance, consideration, and mutual asset with respect to data security." Response at 32.

It may be helpful to begin the analysis of Premera's Motion against Plaintiffs' Fifth Claim with a clarification of terminology and some basic principles of contract law. When parties manifest their agreement by words, the contract is said to be "express." When parties manifest their agreement by conduct, rather than by words, the contract is said to be "implied in fact." A contract implied in fact is still a contract. An express contract and a contract implied in fact are both contracts formed by a mutual manifestation of assent; the only material difference is the form or proof of the mutual assent. A contract implied in law, however, is not a contract. Instead, when an obligation is imposed by law in order to do justice under the facts of a particular situation, even though no promise was ever made or intended, that is called a "contract implied in law." A contract implied in law also may be called a "quasi-contract." The confusing use of the word "contract" in the non-contractual obligation imposed by law in a "contract implied by law" (or a quasi-contract) is simply the result of an historical, procedural quirk. Because the early common law did not contain a writ for the obligation now known as a "contract implied in law," early common law courts permitted the use of the contractual writ of assumpsit and permitted the pleading of a "fictitious" promise. Thus, the non-contractual

obligation of a contract implied in law was treated procedurally as if it were a contract. Further, the principal function of this quasi-contract is to prevent unjust enrichment.[19]

Finally, returning to the concept of a true contract, whether express or implied in fact, under certain circumstances, a court may add or supply an omitted essential term. As explained in the RESTATEMENT (SECOND) OF CONTRACTS:

> When the parties to a bargain sufficiently defined to be a contract have not agreed with respect to a term which is essential to a determination of their rights and duties, a term which is reasonable in the circumstances is supplied by the court.

RESTATEMENT (SECOND) OF CONTRACTS, § 204; *see also* RESTATEMENT (SECOND) OF CONTRACTS, § 204 cmt. d (discussing "supplying a term"); Eyal Zamir, *The Inverted Hierarchy of Contract Interpretation and Supplementation*, 97 COLUM. L. REV. 1710, 1718-19 (1997) (discussing the applicability of RESTATEMENT (SECOND) OF CONTRACTS, § 204 to omitted terms).

When a court supplies an omitted essential term into a contract, the supplied term is sometimes referred to as an "implied" term. Today, one of the most common of such "implied" terms is the implied covenant of good faith and fair dealing, which is recognized as an implied term in all (or almost all) common law contracts. In addition, the pedigree of the doctrine of implying an omitted essential term can be traced at least as far back as the opinion of then-Judge Benjamin Cardozo writing for the New York Court of Appeals in *Wood v. Lucy, Lady Duff-Gordon*, 222 N.Y. 88, 118 N.E. 214 (1917). In that case, the plaintiff had facilities for promoting the sale of women's apparel and entered into an agreement with the defendant, a creator of fashions. An employment agreement was signed by both parties and had many recitals. The defendant, however, argued that it lacked the elements of a contract because it did not bind the

[19] *See generally* John D. Calamari and Joseph M. Perillo, THE LAW OF CONTRACTS at § 1-12, 19-20 (1977); RESTATEMENT (SECOND) OF CONTRACTS, § 4 cmt. a.

plaintiff to anything specific. The Court, however, implied a promise that the plaintiff would use reasonable efforts to market the defendant's designs. As explained by then-Judge Cardozo:

> It is true that he does not promise in so many words that he will use reasonable efforts to place the defendant's indorsements and market her designs. We think, however, that such a promise is fairly to be implied. The law has outgrown its primitive stage of formalism when the precise word was the sovereign talisman, and every slip was fatal. It takes a broader view to-day. A promise may be lacking, and yet the whole writing may be 'instinct with an obligation,' imperfectly expressed (SCOTT, J., in *McCall Co. v. Wright*, 133 App. Div. 62; *Moran v. Standard Oil Co.*, 211 N. Y. 187, 198). If that is so, there is a contract.

*Lucy, Lady Duff-Gordon*, 222 N.Y. at 90-91.

Returning now to Premera's challenge to Plaintiffs' Fifth Claim, it is unclear to the Court whether Plaintiffs are alleging the existence of two distinct contracts, one express and the other implied in fact.[20] It is also unclear to the Court whether Plaintiffs are alleging breach of a duty reasonably to protect Sensitive Information as an implied term in an express health benefits contract.

In the alternative, Plaintiffs may be attempting to allege that they have two contracts with Premera—one being an express contract for health benefits and a second being an implied in fact contract concerning the reasonable protection of Sensitive Information furnished as part of the relationship created under the first (and express) contract. Washington law recognizes contracts that are implied in fact. As the Supreme Court of Washington explained:

> On at least four occasions, . . . this court has quoted with approval a definition of a contract implied in fact, . . . as follows: "A true implied contract is an agreement of the parties arrived at from their acts and conduct viewed in the light of surrounding circumstances, and not from their words either spoken or written. *Like an express*

[20] The Court does not read Plaintiffs' Fifth Claim as alleging a quasi-contract, or implied in law contract, because that is what Plaintiffs allege in their Sixth Claim (Restitution/Unjust Enrichment).

> *contract, it grows out of the intentions of the parties to the transaction, and there must be a meeting of minds. Such a contract differs from an express contract only in the mode of proof*." (Italics ours.)
>
> Before a court can find the existence of an implied contract in fact, there must be an offer; there must be an acceptance; the acceptance must be in the terms of the offer; it must be communicated to the offeror; there must be a mutual intention to contract, . . . there must be a meeting of the minds of the parties.

*Milone & Tucci, Inc. v. Bona Fide Builders, Inc.*, 49 Wash. 2d 363, 367-68 (1956) (citations omitted) (emphasis in original).

In response to Premera's Motion, Plaintiffs explain that they

> allege that, *in the alternative to the existence of an express contract*, the specific facts and circumstances of the transaction between Premera and the Policyholder Plaintiffs culminated in a meeting of the minds, wherein the parties understood there to be an offer, acceptance, consideration, and mutual assent with respect to data security.

Response at 32 (emphasis added). Plaintiffs also argue that they have adequately pleaded an implied in fact contract. They state:

> Here, the Policyholder Plaintiffs allege that in order to receive health insurance coverage from Premera, they were required to (i) pay and (ii) hand over their Sensitive Information. (Compl. ¶ 176.) Plaintiffs further allege that they would not have agreed to do either act without an understanding that upon providing Premera with their Sensitive Information, Premera was simultaneously agreeing to safeguard it (and Plaintiffs, in turn, understood they were paying for that agreement). (*Id*. ¶¶ 9, 129.) And finally, Plaintiffs point to Premera's own privacy documents to support that a meeting of the minds occurred—i.e., Premera understood that, by accepting Plaintiffs' payments and Sensitive Information, it was agreeing (and being paid) to protect it. (*Id*. ¶¶ 4-5.) These facts are more than sufficient to establish the existence of an implied contract, which Premera breached by failing to safeguard Plaintiffs' Sensitive Information.

*Id.* at 32-33.

When Plaintiffs argue that their alleged implied in fact contract is "in the alternative to the *existence* of an express contract," it is unclear whether they are pleading the existence of only one contract (an implied in fact contract that includes both the purchase of health insurance and the provision of data security) or the existence of two distinct (but perhaps related) contracts, an express contract for the provision of health benefits and a separate implied in fact contract for the provision of data security. Plaintiffs have leave to replead their Fifth Claim to clarify this issue. As previously stated, Plaintiffs also have leave to replead to clarify whether they are alleging, in the further alternative, breach of a duty reasonably to maintain the security of Sensitive Information as an implied term in an otherwise express contract for health benefits.

**3. Plaintiffs' Sixth Claim (Restitution/Unjust Enrichment)**

In their Sixth Claim, the Policyholder Plaintiffs allege that "they conferred a monetary benefit on Defendant in the form of fees paid for healthcare insurance," that a portion of these fees "were supposed to be used by Defendant, in part, to pay for the administrative costs of data management and security," that "Defendant did not use such fees to pay for the administrative costs of data management and security," and that "as a result of Defendant's conduct, Plaintiffs . . . suffered actual damages in an amount equal to the difference in the free-market value of the secure healthcare insurance for which they paid and the insecure healthcare insurance they received." Compl. ¶ 187-90.

Premera argues that Plaintiffs' complaint does not allege any facts to explain how they bargained for data security or how some portion of their premium to Premera was supposed to be allocated to data security. Premera also argues that Plaintiffs' unjust enrichment theory also fails because it is tethered to their allegations of fraud without any allegations of reliance on the allegedly false statements.

In response, Plaintiffs argue that under Washington law, "[a] party claiming unjust enrichment must prove three elements: (1) the defendant receive[d] a benefit, (2) the received benefit is at the plaintiff's expense, and (3) the circumstances ma[d]e it unjust for the defendant to retain the benefit without payment." *Austin v. Ettl*, 286 P.3d 85, 96 (Wash. 2012) (citation omitted). Plaintiffs add that Oregon and Alaska laws are similar, citing *Wilson v. Gutierrez*, 323 P.3d 974, 978 (Or. App. 2014) (reciting similar elements under Oregon law); *Darling v. Standard Alaska Prod. Co.*, 818 P.2d 677, 680 (Alaska 1991) (reciting similar elements under Alaska law). Plaintiffs also cite the data breach case of *Resnick*, in which the Eleventh Circuit reversed the district court's dismissal of the plaintiffs' unjust enrichment claim under Florida law. *Resnick*, 693 F.3d at 1328. Similarly, Judge Koh in *Anthem* found comparable allegations of unjust enrichment sufficient to withstand a motion to dismiss under New York law. *Anthem*, 2016 WL 3029783, at *27-29.

Plaintiffs allege that they made payments to Premera and that under the circumstances it is unjust for Premera to retain the benefits received without payment. This is sufficient to withstand a motion to dismiss.

**C. Plaintiffs' Ninth Claim (California CMIA)**

In their Ninth Claim, Plaintiffs allege, on behalf of Plaintiff Hansen-Bosse and a statewide California statutory class, that Premera violated California's CMIA. Plaintiffs allege that the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information, Cal. Civ. Code § 56.36 (2013), and requires that an entity such as Premera that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." *Id.* § 56.101(a).

Premera argues that Plaintiff Hansen-Bosse, who is the only named Plaintiff to assert a claim under the CMIA, fails to state a claim under that statute. According to Premera, a plaintiff asserting a claim under the CMIA

> must allege as a threshold matter that an "unauthorized person has actually viewed the [plaintiff's] stolen records[.]" *Sutter Health v. Superior Court*, 174 Cal. Rptr. 3d 653, 656 (Cal. Ct. App. 2014); *see also Regents of Univ. of California v. Superior Court*, 163 Cal. Rptr. 3d 205, 221 (Cal. Ct. App. 2013) (same). And under the CMIA, a viewing of non-medical personal information is not enough; the unauthorized person must have actually viewed the plaintiff's confidential medical information, *i.e.*, information "relating to medical history, mental or physical condition, or treatment of the individual." *Eisenhower Med. Ctr. v. Superior Court*, 172 Cal. Rptr. 3d 165, 170 (Cal. Ct. App. 2014). The facts must also support the conclusion that an unauthorized viewing of confidential medical information occurred, without resorting to "layers of speculation." *See Regents*, 163 Cal. Rptr. 3d at 221 n.15.

Motion at 24. According to Premera, Ms. Hansen-Bosse has not met these requirements.

In response, Plaintiffs argue that medical information within the meaning of the CMIA was disclosed in the data breach, "including clinical information." Plaintiffs assert that they have alleged that the information that the hackers acquired in the data breach—including medical information—has not only been "viewed" by the hackers, but that it already has been misused in a variety of ways to harm class members including, to date, a number of fraudulently filed tax returns and fraudulent attempts to open lines of credit in victims' names. Response at 39-40 (citing Compl. ¶¶ 78-100).

In its Reply, Premera notes that Plaintiff Hansen-Bosse does not dispute that she must plausibly allege some unauthorized party "actually viewed" her confidential medical information to state a claim under the California CMIA. Reply at 21. Premera adds that "there are no allegations that would support the conclusion that any information has been disclosed 'to public

view.' In fact, as Premera disclosed in its notification, it is not clear that any information was actually accessed or removed from Premera's systems." *Id.*

Ms. Hansen-Bosse alleges that she received a letter from Premera notifying her that her personal information may have been compromised. Compl. ¶ 81. She also alleges that in May 2015 she discovered on her credit report an inquiry for a car loan that she did not recognize and that her checking account was fraudulently accessed around the same time period. *Id.* Plaintiffs also allege that "[a]s a direct and proximate result of Defendant's negligence, it disclosed and released Plaintiffs' and the Statewide California Statutory Class members' Sensitive Information to hackers." Compl. ¶ 216. In addition, the Complaint defines "Sensitive Information" as including medical claims information and other protected health information as defined by HIPAA. Compl. ¶ 1. This is sufficient to withstand a motion to dismiss.

**D. Plaintiffs' Tenth Claim (Breach of Fiduciary Duty)**

In their Tenth Claim, Plaintiffs allege that "[i]n requiring Plaintiffs . . . to submit Sensitive non-public personal health and financial information in order to obtain coverage under a health insurance policy and/or receive treatment in the Blue Cross Blue Shield network, Premera placed itself in a position of trust with respect to such Sensitive non-public personal health and financial information." Compl. ¶ 219. Plaintiffs also allege that "[t]his position of trust was enhanced by Premera's necessary involvement in the fiduciary relationship between doctors and their patients, and by Premera's own fiduciary or quasi-fiduciary relationship as an insurer to its insured." Compl. ¶ 220. Plaintiffs further allege that Premera's "position of trust" also arises or is enhanced by certain duties imposed by federal law, specifically HIPAA and Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Compl. ¶¶ 221-22. Plaintiffs then allege that Premera breached its fiduciary duties that it owed to Plaintiffs by failing to use

sufficient measures to protect Plaintiffs' Sensitive Information from hacking and by failing to provide timely notice of the breach at issue in this case. Compl. ¶ 224.

Premera moves to dismiss Plaintiffs' breach of fiduciary duty claim, arguing that it owed no fiduciary duties to Plaintiffs as a matter of law. According to Premera, courts have routinely rejected a "guardian of personal information" theory as a basis for imposing a fiduciary duty. *See Cooney v. Chicago Public Schools*, 943 N.E.2d 23, 29 (Ill. App. Ct. 2010); *Anderson v. Hannaford Bros.*, 659 F.3d 151, 157 (1st Cir. 2011); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 427 F. Supp. 2d 526, 534 (M.D. Pa. 2006), *aff'd*, 533 F.3d 162 (3d Cir. 2008).[21]

In response, Plaintiffs assert that Washington state law recognizes two categories of fiduciary duty. According to Plaintiffs, a fiduciary duty as a matter of law exists where "the nature of the relationship between the parties is historically considered fiduciary in character[.]" *Alexander v. Sanford*, 325 P.3d 341, 363 (Wash. Ct. App. 2014) (quoting *McCutcheon v. Brownfield*, 467 P.2d 868 (Wash. 1970)). Second, according to Plaintiffs, even where a fiduciary duty as a matter of law does not exist, "a fiduciary relationship arises in fact when there is something in the particular circumstances which approximates a business agency, a professional relationship, or a family tie, something which itself impels or induces the trusting party to relax the care and vigilance which he otherwise should, and ordinarily would, exercise." *Id*. (quoting *Hood v. Cline*, 212 P.2d 110 (Wash. 1949)). Plaintiffs argue that this type of fiduciary

[21] In addition, as Premera also argues, although Plaintiffs also allege that under Washington law a fiduciary duty may arise from the "quasi-fiduciary" relationship between an insurer and insured (Compl. ¶ 220), "no Washington court has recognized a claim for breach of fiduciary duty by an insured." *Beasley v. State Farm Mut. Auto. Ins. Co.*, 2014 WL 1494030, at *7 (W.D. Wash. Apr. 16, 2014); *see also, e.g.*, *Vail v. Country Mut. Ins. Co.*, 2015 WL 2207952, at *7 (D. Or. May 11, 2015) (Oregon law) ("Contrary to plaintiffs' assertion, an insurer is not in a fiduciary relationship with its insured.").

relationship may exist where one party has superior knowledge and thereby induces reliance on that knowledge by the other party. *Pope v. Univ. of Wash.*, 852 P.2d 1055, 1063 (Wash. 1993).

Plaintiffs' arguments are not persuasive. First, the nature of the relationship between the parties is not the type of relationship that historically has been considered fiduciary in character. Second, Plaintiffs have not alleged that they have been induced to relax the care and vigilance that they otherwise should, and ordinarily would, exercise concerning their confidential information. Plaintiffs' primary argument appears to be that had Plaintiffs known how Premera actually would be treating their Sensitive Information, they would not have entered into any relationship with Premera. That may or may not support a claim other than breach of fiduciary duty, but it is insufficient to establish a fiduciary relationship.

**E. The Filed-Rate Doctrine**

In its Motion, Premera argues that Plaintiffs' claims for "overpayment damages" are barred as a matter of law by the filed-rate doctrine. Motion at 26-27. Premera primarily relies upon *McCarthy Finance, Inc. v. Premera*, 347 P.3d 872, 873 (Wash. 2015). According to Premera, the plaintiffs in *McCarthy* alleged that Premera and another defendant made false and misleading representations to the plaintiffs that induced the plaintiffs to purchase health insurance policies under false pretenses. These plaintiffs sought disgorgement damages based on the sum of the excess premiums paid to the defendants. The Washington Supreme Court held that the plaintiffs' claim was barred because "the court would need to determine what health insurance premiums would have been reasonable for the Policyholders to pay as a baseline for calculating the amount of damages and the [Office of the Insurance Commissioner] has already determined that the health insurance premiums paid by the Policyholders were reasonable." *McCarthy*, 347 P.3d at 876. Premera argues that the same analysis applies here.

Plaintiffs respond that, unlike in *McCarthy*, the Policyholder Plaintiffs here do not allege that Premera made any excessive overcharges for premiums. "Rather, Plaintiffs allege that Premera wrongfully charged them for a service (cyber security) that was not provided." Response at 23.

In their Sixth Claim, however, which alleges Restitution/Unjust Enrichment, Plaintiffs assert that the class "suffered actual damages in an amount equal to the difference in the free-market value of the secure healthcare insurance for which they paid and the insecure healthcare insurance they received." Compl. ¶ 190. The Court is skeptical that these damages can be measured in a way that does not violate the filed-rate doctrine. Notwithstanding this skepticism, the Court believes that the better practice is to address this issue at summary judgment or trial, rather than at the pleading stage.

**F. Premera's Challenges to Plaintiffs' Causation Allegations**

In its Motion, Premera argues that Plaintiffs' alleged "overpayment damages" are not recoverable on their contract, tort, and statutory unfairness claims because they are not causally connected to the alleged breach of duty that Plaintiffs assert in support of their claims. Motion at 27-28. Premera also argues that many of the named Plaintiffs failed adequately to plead that their alleged economic damages were caused by the cyberattack on Premera. *Id*. at 32.

Plaintiffs respond that the Policyholder Plaintiffs allege more "traditional" data breach damages, *e.g.* out-of-pocket expenses relating to fraudulent accounts and efforts to mitigate further injury, and that Policyholder Plaintiffs would not have purchased insurance policies from Premera had they known about Premera's actual data security practices (*i.e.*, "benefit of the bargain" damages for the Policyholder Plaintiffs). Response at 20-21.

Plaintiffs' several theories of damages are becoming generally accepted in the emerging area of data breach litigation. *See, e.g.*, *Anthem*, 2016 WL 3029783, at *12-16 (discussing benefit

of the bargain losses, loss of value of personal information, and consequential out of pocket damages); *In re Target*, 2014 WL 7192478, at *22-23 (accepting damages theory alleging that plaintiffs "would not have shopped" had they known about the Target's data security issues); *Resnick*, 693 F.3d at 1328 (endorsing benefit of the bargain damages in data breach case on unjust enrichment claim, on allegations that health insurer failed to use money for data security in accordance with privacy notices); *Weinberg v. Advanced Data Processing, Inc.*, 2015 WL 8098555, at *6 (S.D. Fla. Nov. 17, 2015) (following *Resnick* in data breach case against medical payment processor); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1105 (N.D. Cal. 2010) (allowing benefit of the bargain damages in case involving public disclosure of sensitive information from AOL); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014) (denying motion to dismiss where plaintiffs alleged they paid more for Adobe products than they would have paid had they known that Adobe was not providing the reasonable security it represented).

In addition, in *Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688, 690-91 (7th Cir. 2015), the data security breach plaintiffs alleged: (1) a temporal element (*i.e.*, that they "incurred fraudulent charges on [their credit or debit accounts] after [they] used [them] at Neiman Marcus"); (2) that Neiman Marcus notified them that their data had been compromised; and (3) that Neiman Marcus offered them "one year of free credit monitoring and identity-theft protection." *Remijas*, 794 F.3d at 690-91. In addressing whether the plaintiffs had alleged a plausible connection between the data breach and their alleged damages, the Seventh Circuit explained:

> The fact that Target or some other store might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. . . . It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might

> have been exposed and that it contacted members of the class to tell them they were at risk. Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level.

*Id.* at 696 (citations omitted); *see also Anthem*, 2016 WL 3029783, at *15-16.

At this stage of the litigation, Plaintiffs have sufficiently alleged causation.

**G. Plaintiffs Who Claim Delayed Notification, But Fail to Allege Intervening Misuse**

In their Second and Eighth Claims, Plaintiffs allege that Premera violated various state data breach notification laws by unreasonably delaying notification of the breach. Compl. ¶¶ 143, 209-210. Premera argues that the only potential damages that could result from this delay would be damages flowing from an actual misuse of the information in the interim, which only three plaintiffs even attempt to allege, according to Premera. Compl. ¶¶ 92, 96, 98. According to Premera, the remaining twenty-five named Plaintiffs have not alleged any injury causally connected to this alleged delayed notification, and their delayed notification claims should be dismissed. Motion at 28.

In response, Plaintiffs identify several named Plaintiffs among the twenty-five identified by Premera who allegedly have suffered damages relating to their taxes. Response at 41. In addition, Plaintiffs argue that even if they cannot recover money damages under the relevant state data breach laws for certain Plaintiffs, those Plaintiffs still would be entitled to seek injunctive relief under the relevant statutes. *Id.* at 42. Plaintiffs are correct. *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) (denying motion to dismiss, reasoning that "Plaintiffs may pursue their injunctive relief claims under [Cal. Civ. Code] Section 1798.84(e), which affords relief when a 'business violates, proposes to violate, or has violated' the [CRA].'"). Accordingly, it would be inappropriate to

dismiss Plaintiffs' Second and Eighth Claims, even for those Plaintiffs who suffered no intervening misuse.

**H. Plaintiffs Who Claim Only Time and Expense Mitigating Possible Future Harm**

Premera argues that seven of the named Plaintiffs do not allege that their own personal information has been misused, and instead seek damages based solely on their alleged time and effort "addressing issues arising from the Premera Breach" and, in one instance, from the alleged purchase of credit monitoring services. Compl. ¶¶ 79, 84, 86-88. Premera asserts that these damages are not cognizable. Motion at 29.

Plaintiffs respond that no Plaintiff seeks damages solely based on his or her alleged time and effort addressing issues arising from the Premera breach. Instead, all Plaintiffs seek damages based on a "benefit of the bargain" theory and a theory of the lost economic value of their Sensitive Information. Many Plaintiffs also seek damages based on actual out of pocket expenditures. Premera may be correct that some Plaintiffs seek damages based on the value of their time expended in mitigating possible future harm. At least one court appears to have accepted that damage theory. *See Kuhn v. Capital One Fin. Corp.*, 2006 WL 3007931, at *3 (Mass. App. Ct. 2006) (holding that time spent attempting to undo actual identity theft is compensable). Whether that particular damage theory is sound or whether that particular damages theory is state-specific are not issues that need to be resolved at this stage of the litigation.

**CONCLUSION**

Premera's Motion to Dismiss (ECF 49) is GRANTED IN PART AND DENIED IN PART. Plaintiffs have insufficiently alleged fraud by affirmative misrepresentation, active concealment, or omission. Plaintiffs also have insufficiently alleged breach of express contract and breach of implied contract. Plaintiffs further have insufficiently alleged breach of fiduciary

duty by failing adequately to allege the existence of a fiduciary relationship. Plaintiffs have sufficiently alleged unjust enrichment, violation of the California Confidentiality of Medical Information Act, causation, and damages. Plaintiffs have leave to file a Second Consolidated Class Action Complaint consistent with this Opinion and Order.

**IT IS SO ORDERED.**

DATED this 1st day of August, 2016.

/s/ Michael H. Simon
Michael H. Simon
United States District Judge